**IN THE UNITED STATES DISTRICT COURT**
**FOR THE NORTHERN DISTRICT OF ILLINOIS**
**EASTERN DIVISION**

| | | |
|---|---|---|
| LLOYD GARCIA and KARLA GARCIA, *on behalf of themselves and all others similarly situated,* | § | |
| | § | CASE NO. 1:24-cv-10973 |
| Plaintiffs, | § | |
| vs. | § | JURY TRIAL DEMANDED |
| ABBOTT LABORATORIES EMPLOYEES CREDIT UNION, | § | |
| Defendant. | § | |

**ORIGINAL COMPLAINT—CLASS ACTION**

Plaintiffs Lloyd Garcia and Karla Garcia ("Plaintiffs"), individually and on behalf of all others similarly situated, sue Defendant Abbott Laboratories Employees Credit Union ("ALEC" or "Defendant"), to obtain damages, restitution, and injunctive relief for the Class, as defined below, from Defendant. Plaintiffs make the following allegations upon information and belief, except as to their own actions, the investigation of their counsel, and the facts that are a matter of public record.

## INTRODUCTION

1. This class action arises out of the recent data security incident and data breach that was perpetrated against Defendant (the "Data Breach"), which held in its possession certain personally identifiable information ("PII" or the "Private Information") of Plaintiffs and other current and former customers of Defendant, the putative class members ("Class"). This Data Breach occurred on August 2, 2024.

2. The Private Information compromised in the Data Breach included certain personal information of Defendant ALEC's customers, including Plaintiffs.

3. Defendant has reported to the Maine Attorney General's office that the personal information of 36,044 individuals was affected in the data breach.[1]

4. The Data Breach resulted from Defendant's failure to implement adequate and reasonable cyber-security procedures and protocols necessary to protect individuals' Private Information with which it was entrusted for business relationships.

5. Plaintiffs bring this class action lawsuit on behalf of those similarly situated to address Defendant's inadequate safeguarding of Class Members' Private Information that it collected and maintained, and for failing to provide timely and adequate notice to Plaintiffs and other Class Members that their information was subjected to unauthorized access by an unknown third party and precisely what type of information was accessed.

6. Defendant maintained the Private Information in a reckless manner. In particular, the Private Information was maintained on Defendant's computer network in a condition vulnerable to cyberattacks. Upon information and belief, the mechanism of the Data Breach and potential for improper disclosure of Plaintiffs' and Class Members' Private Information was a known risk to Defendant, and thus Defendant was on notice that failing to take steps necessary to secure the Private Information from those risks left that property in a dangerous condition.

7. Defendant, through its employees, disregarded the rights of Plaintiffs and Class Members (defined below) by, among other things, intentionally, willfully, recklessly, or negligently failing to take adequate and reasonable measures to ensure its data systems were protected against unauthorized intrusions. Defendant also failed to disclose that it did not have adequately robust computer systems and security practices to safeguard Plaintiffs' and Class

[1] Office of the Maine Attorney General, Data Breach Notifications, *available at* https://www.maine.gov/ag/consumer/identity_theft/index.shtml (*last accessed* October 23, 2024).

Members' Private Information and failed to take standard and reasonably available steps to prevent the Data Breach.

8. In addition, Defendant failed to properly monitor the computer network and systems that housed the Private Information. Had Defendant's employees (presumably in the IT department) properly monitored its property, it would have discovered the intrusion sooner.

9. Plaintiffs' and Class Members' identities are now at risk because of Defendant's negligent conduct since the Private Information that Defendant collected and maintained is now in the hands of data thieves.

10. Armed with the Private Information accessed in the Data Breach, data thieves can commit a variety of crimes. These crimes include opening new financial accounts in Class Members' names, taking out loans in Class Members' names, using Class Members' information to obtain government benefits, filing fraudulent tax returns using Class Members' information, filing false medical claims using Class Members' information, obtaining driver's licenses in Class Members' names but with another person's photograph, and giving false information to police during an arrest.

11. Because of the Data Breach, Plaintiffs and Class Members have been exposed to a heightened and ongoing risk of fraud and identity theft. Plaintiffs and Class Members must now and in the future closely monitor their financial accounts to guard against identity theft.

12. Plaintiffs and Class Members may also incur out of pocket costs for, *e.g.*, purchasing credit monitoring services, credit freezes, credit reports, or other protective measures to deter and detect identity theft.

13. Through this Complaint, Plaintiffs seek to remedy these harms on behalf of himself and all similarly situated individuals whose Private Information was accessed during the Data Breach.

14. Plaintiffs seek remedies including, but not limited to, compensatory damages, reimbursement of out-of-pocket costs, and injunctive relief including improvements to Defendant's data security systems, future annual audits, and adequate credit monitoring services funded by Defendant.

15. Accordingly, Plaintiffs sue Defendant seeking redress for their unlawful conduct, and asserting claims for: (i) negligence, (ii) negligence *per se*, and (iii) breach of implied contract.

## PARTIES

16. Plaintiff Lloyd Garcia is and at all times mentioned herein was an individual citizen of Illinois, residing in the city of Highland Park.

17. Plaintiff Karla Garcia is and at all times mentioned herein was an individual citizen of Illinois, residing in the city of Highland Park.

18. Plaintiffs provided Defendant with their sensitive PII as part of the process of opening accounts with ALEC. Plaintiffs received notice of the Data Breach around October 18, 2024, informing them that their sensitive information was part of Defendant's Data Breach. A copy of the notices provided to Plaintiffs is attached hereto as **Exhibit A**.

19. Defendant ALEC is an Illinois not-for-profit company with its principal place of business at 325 Tri-State Parkway, Gurnee, Illinois 60031.

## JURISDICTION AND VENUE

20. This Court has subject matter jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). The amount in controversy exceeds $5 million, exclusive of interest and costs. The number of class members exceeds 100, many of whom have different citizenship from Defendant. Thus, minimal diversity exists under 28 U.S.C. § 1332(d)(2)(A).

21. This Court has personal jurisdiction over Defendant because it operates and is headquartered in this District and conducts substantial business in this District.

22. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(a)(l) because a substantial part of the events giving rise to this action occurred in this District. Moreover, Defendant is based in this District, maintains Plaintiffs' and Class Members' Private Information in this District, and has caused harm to Plaintiffs and Class Members in this District.

## FACTUAL ALLEGATIONS

### *Defendant's Business*

23. Defendant is a member-owned credit union that offers financial services to members throughout the United States.

24. In the ordinary course of applying for an account with ALEC, each customer must provide (and Plaintiffs did provide) Defendant with sensitive, personal, and private information, including his or her Social Security number and contact information.

25. Defendant agreed to and undertook legal duties to maintain the Private Information entrusted to it by Plaintiffs and Class Members safely, confidentially, and in compliance with all applicable laws.

26. The customer information held by Defendant in its computer system and network included the Private Information of Plaintiffs and Class Members.

### *The Data Breach*

27. A Data Breach occurs when cyber criminals intend to access and steal Private Information that has not been adequately secured by a business entity like Defendant.

28. According to Defendant's October 18, 2024, notice letter to Plaintiff Lloyd Garcia (Exhibit A),

> We recently learned that an unknown, unauthorized third party gained access to one ALEC employee email account. Upon discovering the incident, we promptly secured the email account and began an internal investigation. We also engaged a forensic security firm to investigate and confirm the security of our email systems The investigation determined that

> an unauthorized third party accessed the email account on August 2, 2024, and may have acquired certain information contained in the account.
> . . .
> We reviewed the contents of the involved email account to determine if it contained any personal information that may have been viewed or acquired by the third party. On September 23, 2024, we completed our review and determined that the email account contained some of your personal information, including your name in combination with your financial account number and Social Security number.

29. Defendant had obligations created by contract, industry standards, common law, and representations made to Class Members, to keep Class Members' Private Information confidential and to protect it from unauthorized access and disclosure.

30. Plaintiffs and Class Members provided their Private Information to Defendant with the reasonable expectation and mutual understanding that Defendant would comply with its obligations to keep such information confidential and secure from unauthorized access.

31. Defendant was or should have been aware of the significant risk that cybercriminals would attempt to steal Plaintiffs' and Class Members' Private Information.

32. As reported by the Identity Theft Resource Center, in 2023 a record 3,205 data breaches occurred, resulting in around 353,027,892 individuals' information being compromised, a 78% increase from 2022.[2] Of the 2023 recorded data breaches, 744 of them, or 23%, were in the financial services industry.[3]

33. Therefore, the increase in such attacks, and attendant risk of future attacks, was widely known to the public and to anyone in Defendant's industry, including Defendant.

[2] *See* Identity Theft Resource Center, *2023 Data Breach Report* (January 2024), *available at* https://www.idtheftcenter.org/publication/2023-data-breach-report/ (last visited September 19, 2024).
[3] *Id.*

***Defendant Failed to Comply with FTC Guidelines***

34. The Federal Trade Commission ("FTC") has promulgated many guides for businesses which show how important it is to implement reasonable data security practices. According to the FTC, the need for data security should shape all business decision-making.

35. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established cyber-security guidelines for businesses. The guidelines note that businesses should protect the personal information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct any security problems.[4] The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor incoming traffic for activity suggesting someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.[5]

36. The FTC further recommends that companies not maintain PII longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.

37. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect client data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an

[4] Federal Trade Commission, *Protecting Personal Information: A Guide for Business* (2016), *available at* www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last visited August 19, 2024).
[5] *Id.*

unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions also clarify the measures businesses must take to meet their data security obligations.

38. Defendant failed to properly implement basic data security practices. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to customers' PII constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

39. Defendant was always fully aware of its obligation to protect the PII of its customers. Defendant was also aware of the significant repercussions that would result from its failure to do so.

***Defendant Failed to Comply with Industry Standards***

40. As shown above, financial institutions are widely known to be particularly vulnerable to cyberattacks because of the value of the PII which they collect and maintain.

41. Several best practices have been identified that at a minimum should be implemented by employers like Defendant, including, but not limited to, educating all employees; strong passwords; multi-layer security, including firewalls, antivirus, and antimalware software; encryption, making data unreadable without a key; multi-factor authentication; backup data; and limiting which employees can access sensitive data.

42. Other best cybersecurity practices that are standard include installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches and routers; monitoring and protection of physical security systems; protection against any possible communication system; training staff regarding critical points.

43. Defendant failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework Version 1.1 (including, without limitation, PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

44. These foregoing frameworks are existing and applicable industry standards for any business that handles and stores large volumes of sensitive information, and Defendant failed to comply with these accepted standards, thereby opening the door to and causing the Data Breach.

## DEFENDANT'S BREACH

45. Defendant breached its obligations to Plaintiffs and Class Members and/or was otherwise negligent and reckless because it failed to properly maintain and safeguard its computer systems and its data. Defendant's unlawful conduct includes, but is not limited to, the following acts and/or omissions:

a. Failing to maintain an adequate data security system to reduce the risk of data breaches and cyber-attacks;

b. Failing to adequately protect customers' Private Information;

c. Failing to properly monitor its own data security systems for existing intrusions;

d. Failing to train employees in the proper handling of emails containing how the cyberattackers were able to first access Defendant's networks, and to and maintain adequate email security practices;

e. Failing to put into place proper procedures, software settings, and data security software protections to adequately protect against a blunt force intrusion;

f. Failing to comply with FTC guidelines for cybersecurity, in violation of Section *5* of the FTC Act; and

g. Failing to adhere to industry standards for cybersecurity.

46. As the result of computer systems needing security upgrading, inadequate procedures for handling emails containing ransomware or other malignant computer code, and inadequately trained employees who opened files containing the ransomware virus, Defendant negligently and unlawfully failed to safeguard Plaintiffs' and Class Members' Private Information.

47. Accordingly, as outlined below, Plaintiffs and Class Members now face an increased risk of fraud and identity theft.

***Because of Defendant's Failure to Safeguard Private Information, Plaintiffs and the Class Members Have and Will Experience Substantial Harm in the Form of Risk of Continued Identity Theft.***

48. Plaintiffs and members of the proposed Class have suffered injury from the misuse of their PII that can be directly traced to Defendant.

49. The ramifications of Defendant's failure to keep Plaintiffs' and the Class's PII secure are severe. Identity theft occurs when someone uses another's personal information such as that person's name, account number, Social Security number, driver's license number, date of birth, and/or other information, without permission, to commit fraud or other crimes. According to experts, one out of four data breach notification recipients become a victim of identity fraud.

50. Because of Defendant's failures to prevent—and to timely detect—the Data Breach, Plaintiffs and the proposed Class have suffered and will continue to suffer damages, including monetary losses, lost time, anxiety, and emotional distress. They have suffered or are at an increased risk of suffering:

a. The loss of the opportunity to control how their PII is used;

b. The diminution in value of their PII;

c. The compromise and continuing publication of their PII;

d. Out-of-pocket costs associated with the prevention, detection, recovery, and remediation from identity theft or fraud;

e. Lost opportunity costs and lost wages associated with the time and effort expended addressing and attempting to mitigate the actual and consequences of the Data Breach, including, but not limited to, efforts spent researching how to prevent, detect, contest, and recover from identity theft and fraud;

f. Delay in receipt of tax refund monies;

g. Unauthorized use of stolen PII; and

h. The continued risk to their PII, which remains in the possession of Defendant and is subject to further breaches so long as Defendant fails to undertake the appropriate measures to protect the PII in its possession.

51. Stolen PII is one of the most valuable commodities on the criminal information black market. According to Experian, a credit-monitoring service, stolen PII can be worth up to $1,000.00 depending on the type of information obtained.

52. The value of Plaintiffs' and the proposed Class's PII on the black market is considerable. Stolen PII trades on the black market for years, and criminals often post stolen private information openly and directly on various "dark web" internet websites, making the information publicly available, for a substantial fee of course.

53. It can take victims years to spot identity or PII theft, giving criminals plenty of time to abuse that information for money.

54. One such example of criminals using PII for profit is the development of "Fullz" packages.

55. Cyber-criminals can cross-reference two sources of PII to marry unregulated data available elsewhere to criminally stolen data with an astonishingly complete scope and degree of accuracy to assemble complete dossiers on individuals. These dossiers are known as "Fullz" packages.

56. The development of "Fullz" packages means that stolen PII from the Data Breach can easily be used to link and identify it to Plaintiffs' and the proposed Class's phone numbers, email addresses, and other unregulated sources and identifiers. In other words, even if certain

information such as emails, phone numbers, or credit card numbers may not be included in the PII stolen by the cyber-criminals in the Data Breach, criminals can easily create a Fullz package and sell it at a higher price to unscrupulous operators and criminals (such as illegal and scam telemarketers) over and over. That is exactly what is happening to Plaintiffs and members of the proposed Class, and it is reasonable for any trier of fact, including this Court or a jury, to find that Plaintiffs' and other members of the proposed Class's stolen PII is being misused, and that such misuse is traceable to the Data Breach.

57. According to the FBI's Internet Crime Complaint Center (IC3) 2019 Internet Crime Report, Internet-enabled crimes reached their highest number of complaints and dollar losses that year, resulting in more than $3.5 billion in losses to individuals and business victims, and the numbers are only rising.

58. Further, according to the same report, "rapid reporting can help law enforcement stop fraudulent transactions before a victim loses the money for good" Defendant did not rapidly report to Plaintiffs and the Class that their PII had been stolen.

59. Victims of identity theft also often suffer embarrassment, blackmail, or harassment in person or online, and/or experience financial losses resulting from fraudulently opened accounts or misuse of existing accounts.

60. In addition to out-of-pocket expenses that can exceed thousands of dollars and the emotional toll identity theft can take, some victims must spend a considerable time repairing the damage caused by the theft of their PII. Victims of new account identity theft will likely have to spend time correcting fraudulent information in their credit reports and continuously monitor their reports for future inaccuracies, close existing bank/credit accounts, open new ones, and dispute charges with creditors.

61. Further complicating the issues faced by victims of identity theft, data thieves may

wait years before attempting to use the stolen PII. To protect themselves, Plaintiffs and the Class will need to remain vigilant against unauthorized data use for years or even decades to come.

62. The Federal Trade Commission ("FTC") has also recognized that consumer data is a new and valuable form of currency. In an FTC roundtable presentation, former Commissioner Pamela Jones Harbour stated that "most consumers cannot begin to comprehend the types and amount of information collected by businesses, or why their information may be commercially valuable. Data is currency."[6]

63. The FTC has also issued Many guidelines for businesses that highlight the importance of reasonable data security practices. The FTC has noted the need to factor data security into all business decision-making. According to the FTC, data security requires:

(1) encrypting information stored on computer networks;

(2) retaining payment card information only as long as necessary;

(3) properly disposing of personal information that is no longer needed;

(4) limiting administrative access to business systems;

(5) using industry-tested and accepted methods for securing data;

(6) monitoring activity on networks to uncover unapproved activity;

(7) verifying that privacy and security features function properly;

(8) testing for common vulnerabilities; and

(9) updating and patching third-party software.

64. According to the FTC, unauthorized PII disclosures ravage consumers' finances, credit history and reputation, and can take time, money and patience to resolve the fallout.[7] The

[6] Statement of FTC Commissioner Pamela Jones Harbour-Remarks Before FTC Exploring Privacy Roundtable, (Dec. 7, 2009), http://www.ftc.gov/speeches/harbour/091207privacyroundtable.pdf (last visited October 4, 2024).

[7] *See* Taking Charge, What to Do If Your Identity is Stolen, FTC, at 3 (2012), *available at* https://www.ojp.gov/ncjrs/virtual-library/abstracts/taking-charge-what-do-if-your-identity-stolen (last visited

FTC treats the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5(a) of the FTC Act.

65. Defendant's failure to properly notify Plaintiffs and Class Members of the Data Breach exacerbated Plaintiffs' and Class Members' injury by depriving them of the earliest ability to take appropriate measures to protect their PII and take other necessary steps to mitigate the harm caused by the Data Breach.

## PLAINTIFFS' EXPERIENCE

66. Plaintiff Lloyd Garcia is and at all times mentioned herein was an individual citizen of Illinois, residing in the city of Highland Park.

67. Plaintiff Karla Garcia is and at all times mentioned herein was an individual citizen of Illinois, residing in the city of Highland Park.

68. Plaintiffs Lloyd Garcia and Karla Garcia are a married couple.

69. Plaintiffs were account holders at ALEC, requiring them to provide their Private Information to Defendant.

70. After Plaintiffs provided Private Information, Defendant suffered a Data Breach.

71. Plaintiffs reasonably expected and understood that Defendant would take, at a minimum, industry standard precautions to protect, maintain, and safeguard their Private Information from unauthorized users or disclosure, and would timely notify them of any data security incidents related to the same. Plaintiffs would not have provided their Private Information to Defendant had they known that Defendant would not take reasonable steps to safeguard it.

October 4, 2024).

72. Plaintiffs are very careful about sharing their sensitive PII. They have never knowingly transmitted unencrypted sensitive PII over the internet or any other unsecured source. Plaintiffs also store any documents containing their sensitive information in a safe and secure location or destroy the documents.

73. Plaintiff Lloyd Garcia received a Notice Letter, dated October 18, 2024, stating that his "name in combination with [his] financial account number and Social Security number" were contained in an email account infiltrated by an unauthorized third party. Exhibit A.

74. Plaintiff Karla Garcia received a Notice Letter, dated October 18, 2024, stating that her "name in combination with [her] financial account number" were contained in an email account infiltrated by an unauthorized third party. *Id.* at 2.

75. Because of the Data Breach and at the recommendation of Defendant and its Notice, Plaintiffs made reasonable efforts to mitigate the effect of the Data Breach, including, but not limited to, researching the Data Breach and monitoring their credit and financial statements.

76. Plaintiffs have spent much time responding to the dangers from the Data Breach and will continue to spend valuable time they otherwise would have spent on other activities, including, but not limited to work and recreation.

77. Even with the best response, the harm caused to Plaintiffs cannot be undone.

78. Plaintiffs know that cybercriminals often sell Private Information, and that their PII could be abused months or even years after a data breach.

79. Had Plaintiffs been aware that Defendant's computer systems were not secure, they would not have entrusted Defendant with their personal data.

## PLAINTIFFS' AND CLASS MEMBERS' DAMAGES

80. To date, Defendant has done little to provide Plaintiffs and Class Members with relief for the damages they have suffered because of the Data Breach, including, but not limited

to, the costs and loss of time they incurred because of the Data Breach. Defendant has only offered 12 months of inadequate credit monitoring services, despite Plaintiffs and Class Members being at risk of identity theft and fraud for the remainder of their lifetimes.

81. The 12 months of credit monitoring offered to persons whose Private Information was compromised is wholly inadequate as it fails to provide for the fact that victims of data breaches and other unauthorized disclosures commonly face multiple years of ongoing identity theft and financial fraud.

82. Defendant's credit monitoring advice to Plaintiffs and Class Members places the burden on Plaintiffs and Class Members, rather than on Defendant, to investigate and protect themselves from Defendant's tortious acts resulting in the Data Breach.

83. Plaintiffs and Class Members have been damaged by the compromise of their Private Information in the Data Breach, and by the severe disruption to their lives as a direct and foreseeable consequence of this Data Breach.

84. Plaintiffs' Private Information was compromised and exfiltrated by cyber-criminals as a direct and proximate result of the Data Breach.

85. Plaintiffs were damaged in that their Private Information is in the hands of cyber criminals.

86. As a direct and proximate result of Defendant's conduct, Plaintiffs and Class Members have been placed at an actual, present, immediate, and continuing increased risk of harm from fraud and identity theft.

87. As a direct and proximate result of Defendant's conduct, Plaintiffs and Class Members have been forced to expend time dealing with the effects of the Data Breach.

88. Plaintiffs and Class Members face substantial risk of out-of-pocket fraud losses such as loans opened in their names, medical services billed in their names, tax return fraud, utility bills opened in their names, credit card fraud, and similar identity theft.

89. Plaintiffs and Class Members face substantial risk of being targeted for future phishing, data intrusion, and other illegal schemes based on their Private Information as potential fraudsters could use that information to more effectively target such schemes to Plaintiffs and Class Members.

90. Plaintiffs and Class Members may also incur out-of-pocket costs for protective measures such as credit monitoring fees, credit report fees, credit freeze fees, and similar costs directly or indirectly related to the Data Breach.

91. Plaintiffs and Class Members also suffered a loss of value of their Private Information when it was acquired by cyber thieves in the Data Breach. Many courts have recognized the propriety of loss of value damages in related cases.

92. Plaintiffs and Class Members have spent and will continue to spend significant amounts of time to monitor their financial accounts and records for misuse.

93. Plaintiffs and Class Members have suffered or will suffer actual injury as a direct result of the Data Breach. Many victims suffered ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the Data Breach relating to:

a. Reviewing and monitoring financial and other sensitive accounts and finding fraudulent insurance claims, loans, and/or government benefits claims;

b. Purchasing credit monitoring and identity theft prevention;

c. Placing “freezes” and “alerts” with reporting agencies;

d. Spending time on the phone with or at financial institutions, healthcare providers, and/or government agencies to dispute unauthorized and fraudulent activity in their

name;

e. Contacting financial institutions and closing or modifying financial accounts; and; and

f. Closely reviewing and monitoring bank accounts and credit reports for unauthorized activity for years to come.

94. Moreover, Plaintiffs and Class Members have an interest in ensuring that their Private Information, which is believed to remain in the possession of Defendant, is protected from further breaches by implementing security measures and safeguards, including, but not limited to, making sure that the storage of data or documents containing personal and financial information is inaccessible online and that access to such data is password protected.

95. As a direct and proximate result of Defendant's actions and inactions, Plaintiffs and Class Members have suffered anxiety, emotional distress, and loss of privacy, and are at an increased risk of future harm.

## CLASS ACTION ALLEGATIONS

96. This action is brought and may be properly maintained as a class action pursuant to Rule 23 of the Federal Rules of Civil Procedure.

97. Plaintiffs bring this action on behalf of themselves and on behalf of all other persons similarly situated.

98. Plaintiffs propose the following Class definition, subject to amendment as appropriate:

> **All persons whose Private Information was compromised because of the August 2, 2024 Data Breach (the "Class").**

99. Excluded from the Class are Defendant's officers and directors, and any entity in which Defendant has a controlling interest; and the affiliates, legal representatives, attorneys,

successors, heirs, and assigns of Defendant. Excluded also from the Class are Members of the judiciary to whom this case is assigned, their families and Members of their staff.

100. Plaintiffs reserve the right to amend or modify the class definitions with greater specificity or division after having an opportunity to conduct discovery.

101. Numerosity. The Members of the Class are so numerous that joinder of all of them in a single proceeding is impracticable. The exact number of Class Members is unknown to Plaintiffs now, but Defendant has reported to the Maine Attorney General that 36,044 individuals were affected by the Data Breach.

102. Commonality. There are questions of law and fact common to the Class, which predominate over any questions affecting only individual Class Members. These common questions of law and fact include, without limitation:

a. Whether Defendant unlawfully used, maintained, lost, or disclosed Plaintiffs' and Class Members' Private Information;

b. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

c. Whether Defendant's data security systems prior to and during the Data Breach complied with applicable data security laws and regulations;

d. Whether Defendant's data security systems prior to and during the Data Breach adhered to industry standards;

e. Whether Defendant owed a duty to Class Members to safeguard their Private Information;

f. Whether Defendant breached its duty to Class Members to safeguard their Private Information;

g. Whether Defendant knew or should have known that its data security systems and monitoring processes were deficient;

h. Whether Plaintiffs and Class Members suffered legally cognizable damages from Defendant's misconduct;

i. Whether Defendant failed to provide notice of the Data Breach promptly; and

j. Whether Plaintiffs and Class Members are entitled to damages, civil penalties, punitive damages, and/or injunctive relief.

103. Typicality. Plaintiffs' claims are typical of those of other Class Members because Plaintiffs' Private Information, like that of every other Class member, was compromised in the Data Breach. Plaintiffs' claims are typical of those of the other Class Members because, among other things, all Class Members were injured through the common misconduct of Defendant. Plaintiffs are advancing the same claims and legal theories on behalf of themselves and all other Class Members, and no defenses are unique to Plaintiffs. Plaintiffs' claims and those of Class Members arise from the same operative facts and are based on the same legal theories.

104. Adequacy of Representation. Plaintiffs will fairly and adequately represent and protect the interests of the Members of the Class. Plaintiffs' Counsel is competent and experienced in litigating class actions, including data privacy litigation of this kind.

105. Predominance. Defendant has engaged in a common course of conduct toward Plaintiffs and Class Members, in that all Plaintiffs' and Class Members' data was stored on the same computer systems and unlawfully accessed in the same way. The common issues arising from Defendant's conduct affecting Class Members set out above predominate over any individualized issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

106. Superiority. A Class action is superior to other available methods for the fair and efficient adjudication of the controversy. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a class action, most Class Members would likely find that the cost of litigating their individual claims is prohibitively high and would therefore have no effective remedy.

107. The prosecution of separate actions by individual Class Members would create a risk of inconsistent or varying adjudications with respect to individual Class Members, which would establish incompatible standards of conduct for Defendant. In contrast, the conduct of this action as a class action presents far fewer management difficulties, conserves judicial resources and the parties' resources, and protects the rights of each Class member.

108. Defendant has acted on grounds that apply generally to the Class as a whole, so that class certification, injunctive relief, and corresponding declaratory relief are appropriate on a Class-wide basis.

109. Finally, all members of the proposed Class are readily ascertainable. Defendant has access to Class Members' names and addresses affected by the Data Breach. Class Members have already been preliminarily identified and sent notice of the Data Breach by Defendant.

## CAUSES OF ACTION

### FIRST COUNT
### NEGLIGENCE
### (On Behalf of Plaintiffs and All Class Members)

110. Plaintiffs re-allege and incorporate the above allegations as if fully set forth herein.

111. Defendant required Plaintiffs and Class Members to submit non-public personal information to do business with ALEC.

112. By collecting and storing this data in Defendant's computer property, and sharing it and using it for commercial gain, Defendant had a duty of care to use reasonable means to secure and safeguard its computer property—and Class Members' Private Information held within it—to prevent disclosure of the information, and to safeguard the information from theft. Defendant's duty included a responsibility to implement processes by which it could detect a breach of its security systems in a reasonably expeditious period and to give prompt notice to those affected in the case of a Data Breach.

113. Defendant owed a duty of care to Plaintiffs and Class Members to provide data security consistent with industry standards and other requirements discussed herein, and to ensure that its systems and networks, and the personnel responsible for them, adequately protected the Private Information.

114. Defendant's duty of care to use reasonable security measures arose because of the special relationship that existed between Defendant and Plaintiffs and the Class. That special relationship arose because Plaintiffs and the Class entrusted Defendant with their confidential Private Information, a necessary part of obtaining services from Defendant.

115. In addition, Defendant had a duty to employ reasonable security measures under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data.

116. Defendant further had a duty to use reasonable care in protecting confidential data because Defendant is bound by industry standards to protect confidential Private Information.

117. Defendant breached its duties, and thus was negligent, by failing to use reasonable measures to protect Class Members' Private Information. The specific negligent acts and omissions committed by Defendant include, but are not limited to, the following:

a. Failing to adopt, implement, and maintain adequate security measures to safeguard Class Members' Private Information;

b. Failing to adequately monitor the security of its networks and systems;

c. Failing to periodically ensure that its email system had plans in place to maintain reasonable data security safeguards;

d. Allowing unauthorized access to Class Members' Private Information;

e. Failing to detect timely that Class Members' Private Information had been compromised;

f. Failing to timely notify Class Members about the Data Breach so that they could take appropriate steps to mitigate the potential for identity theft and other damages; and

g. Failing to secure its stand-alone personal computers, such as the reception desk computers, even after discovery of the data breach.

118. It was foreseeable that Defendant's failure to use reasonable measures to protect Class Members' Private Information would result in injury to Class Members. Further, the breach of security was reasonably foreseeable given the known high frequency of cyberattacks and data breaches.

119. It was therefore foreseeable that the failure to adequately safeguard Class Members' Private Information would result in one or more types of injuries to Class Members.

120. Plaintiffs and Class Members are entitled to compensatory and consequential damages suffered because of the Data Breach.

121. Defendant's negligent conduct is ongoing, in that it still holds the Private Information of Plaintiffs and Class Members in an unsafe and unsecure manner.

122. Plaintiffs and Class Members are also entitled to injunctive relief requiring Defendant to (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) provide adequate credit monitoring to all Class Members.

**SECOND COUNT**
**BREACH OF IMPLIED CONTRACT**
**(On Behalf of Plaintiffs and All Class Members)**

123. Plaintiffs re-allege and incorporate the above allegations as if fully set forth herein.

124. When Plaintiffs and Class Members provided their Private Information to Defendant in exchange for Defendant's services, they entered implied contracts with Defendant under which Defendant agreed to reasonably protect such information.

125. Defendant solicited, offered, and invited Class Members to provide their Private Information as part of Defendant's regular business practices. Plaintiffs and Class Members accepted Defendant's offers and provided their Private Information to Defendant.

126. In entering such implied contracts, Plaintiffs and Class Members reasonably believed and expected that Defendant's data security practices complied with relevant laws and regulations and adhered to industry standards.

127. Plaintiffs and Class Members paid money to Defendant with the reasonable belief and expectation that Defendant would use part of its earnings to obtain adequate data security. Defendant failed to do so.

128. Plaintiffs and Class Members would not have entrusted their Private Information to Defendant in the absence of the implied contract between them and Defendant to keep their information reasonably secure.

129. Plaintiffs and Class Members would not have entrusted their Private Information to Defendant in the absence of its implied promise to monitor its computer systems and networks to ensure that they adopted reasonable data security measures.

130. Plaintiffs and Class Members fully and adequately performed their obligations under the implied contracts with Defendant.

131. Defendant breached its implied contracts with Class Members by failing to safeguard and protect their Private Information.

132. As a direct and proximate result of Defendant's breach of the implied contracts, Class Members sustained damages as alleged here, including the loss of the benefit of the bargain.

133. Plaintiffs and Class Members are entitled to compensatory, consequential, and nominal damages suffered because of the Data Breach.

134. Plaintiffs and Class Members are also entitled to injunctive relief requiring Defendant to, e.g., (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) immediately provide adequate credit monitoring to all Class Members.

**THIRD COUNT**
**NEGLIGENCE *PER SE***
**(On Behalf of Plaintiffs and All Class Members)**

135. Plaintiffs re-allege and incorporate the above allegations as if fully set forth herein.

136. Under the Federal Trade Commission Act, 15 U.S.C. § 45, Defendant had a duty to provide fair and adequate computer systems and data security practices to safeguard Plaintiffs' and Class Members' Private Information.

137. Under the Illinois Personal Information Protection Act, 815 ILCS §§ 530/1, *et seq.*, Defendant had a duty to "implement and maintain reasonable security measures to protect those records from unauthorized access, acquisition, destruction, use, modification, or disclosure." 815 ILCS § 530/45.

138. Under the Illinois Personal Information Protection Act, Defendant had a duty to notify Plaintiffs and Class Members of the Data Breach "in the most expedient time possible and without unreasonable delay." 815 ILCS § 530/10.

139. Defendant breached its duties to Plaintiffs and Class Members under Federal and state law by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiffs' and Class Members' Private Information.

140. Defendant's failure to comply with applicable laws and regulations constitutes negligence *per se*.

141. But for Defendant's wrongful and negligent breach of its duties owed to Plaintiffs and Class Members, Plaintiffs and Class Members would not have been injured.

142. The injury and harm suffered by Plaintiffs and Class Members was the reasonably foreseeable result of Defendant's breach of its duties. Defendant knew or should have known that by failing to meet its duties, and that Defendant's breach would cause Plaintiffs and Class Members to experience the foreseeable harms associated with the exposure of their Private Information.

143. As a direct and proximate result of Defendant's negligent conduct, Plaintiffs and Class Members have suffered injury and are entitled to compensatory, consequential, and punitive damages in an amount to be proven at trial.

## PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of himself and the Class described above seeks the following relief:

a. For an Order certifying this action as a class action, defining the Class as requested herein, appointing Plaintiffs and their counsel to represent the Class, and finding that Plaintiffs are proper representatives of the Class requested herein;

b. For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein relating to the misuse and/or disclosure of Plaintiffs' and Class Members' Private Information, and from refusing to issue prompt, complete and accurate disclosures to Plaintiffs and Class Members;

c. For equitable relief compelling Defendant to use appropriate methods and policies related to consumer data collection, storage, and safety, and to disclose with specificity the type of Private Information compromised during the Data Breach;

d. For equitable relief requiring restitution and disgorgement of the revenues wrongfully retained because of Defendant's wrongful conduct;

e. For an Order directing Defendant to pay for not less than ten years of credit monitoring services for Plaintiffs and the Class;

f. For an award of actual damages, compensatory damages, statutory damages, and statutory penalties, in an amount to be determined, as allowable by law;

g. For an award of punitive damages, as allowable by law;

h. For an award of attorneys' fees and costs, and any other expense, including expert witness fees;

i. Pre- and post-judgment interest on any amounts awarded; and

j. Any other relief that this court may deem just and proper.

**JURY TRIAL DEMANDED**

Plaintiffs demand a trial by jury on all claims so triable.

Date: October 24, 2024

Respectfully submitted,

*/s/ Joshua Sanford*

Joshua Sanford
Arkansas Bar No. 2001037
jsanford@eksm.com
**EKSM, LLP**
10800 Financial Centre Pkwy, Suite 510
Little Rock, Arkansas 72211
Telephone: (501) 221-0088
Facsimile: (888) 787-2040

Leigh S. Montgomery (*pro hac vice* forthcoming)
Texas Bar No. 24052214
lmontgomery@eksm.com
**EKSM, LLP**
1105 Milford Street
Houston, Texas 77006
Phone: (888) 350-3931
Fax: (888) 276-3455